Ethical Hacking and Countermeasures
Version 6

Module XXXVII

Bluetooth Hacking

Bluetooth devices easily hacked

Oct 23 2007 01:31 PM

Cape Town - Bluetooth-enabled devices are vulnerable to unscrupulous hackers, an expert warns.

Bluetooth was invented to connect devices such as cellphones, laptops, PCs, printers, digital cameras and video game consoles over a short-range radio frequency, but like any computer network, using Bluetooth can leave you vulnerable.

"Bluetooth hacking techniques vary tremendously. There are various attacks that have proved to be very effective over the last few years. Some of these attacks include making unauthorised calls and transactions, reading and sending SMSs on a target phone, erasing information and downloading personal information such as phone books and access codes," says ICT security expert Dino Covotsos.

Covotsos is MD of **Telspace**, a Johannesburg-based company specialising in managed security services. Telspace routinely makes use of Bluetooth vulnerabilities to test the security level of its corporate clients' networks.

"From our case studies and actual attack and penetration tests, we have often utilised specific Bluetooth attacks to gain further entrance into a network," Covotsos says.

Source: *http://www.fin24.co.za/*

This module will familiarize you with:

- Bluetooth
- Security Issues in Bluetooth
- Attacks in Bluetooth
- Bluetooth Hacking Tools
- Viruses and Worms
- Bluetooth Security Tools

CEH Certified Ethical Hacker

Bluetooth → Bluetooth Hacking Tools

Security Issues in Bluetooth → Viruses and Worms

Attacks in Bluetooth → Bluetooth Security Tools
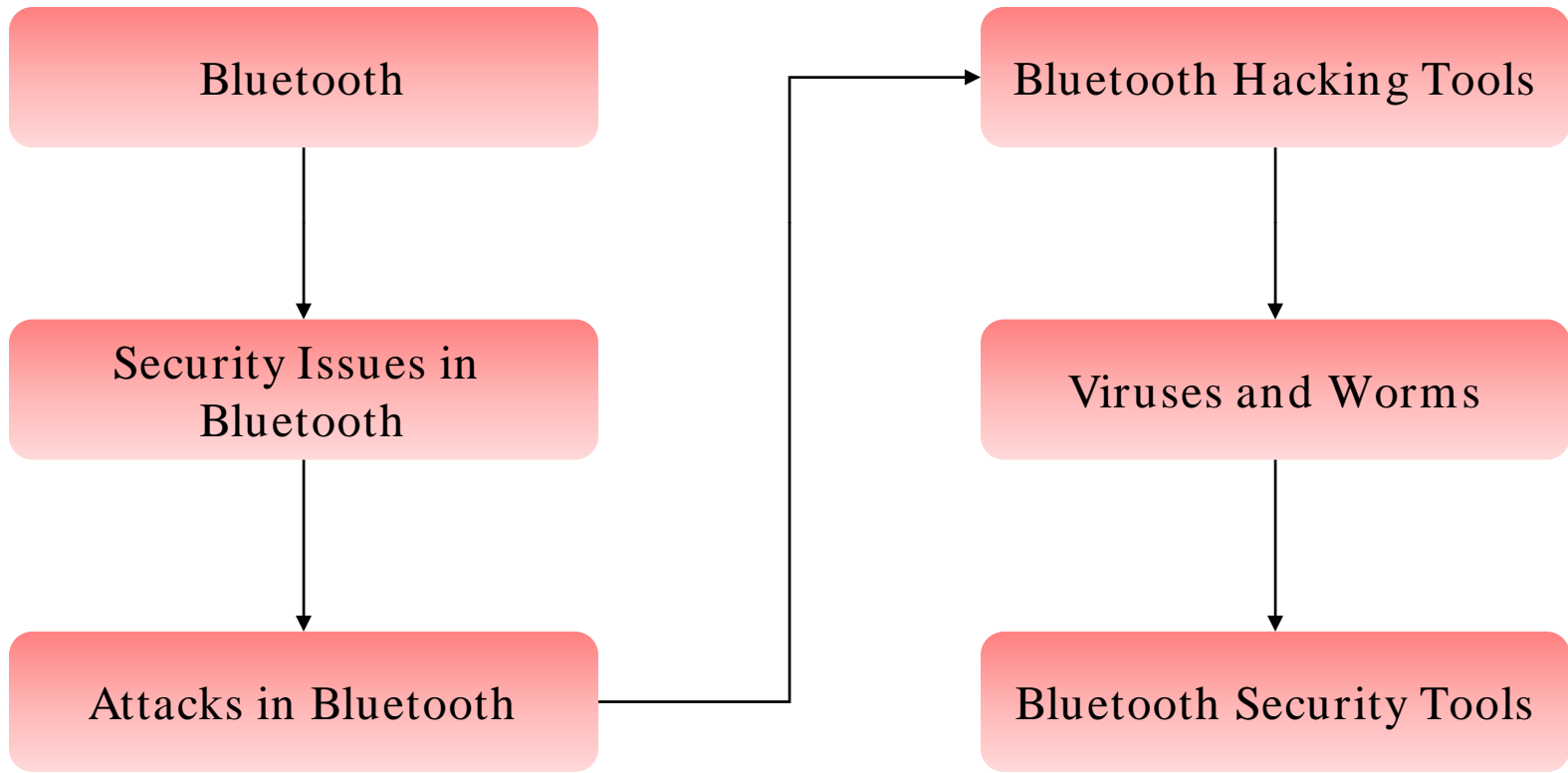
Bluetooth is a short-range wireless communications technology intended to replace the cables connecting portable or fixed devices while maintaining high levels of security

It wirelessly connects mobile phones, portable computers, stereo headsets, MP3 players, and more

Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can connect to other Bluetooth enabled devices in proximity

Bluetooth enabled electronic devices connect and communicate wirelessly through short-range, ad hoc networks known as piconets

Security within Bluetooth itself covers three major areas:

- Authentication
- Authorization
- Encryption

The following are the various security issues in Bluetooth:

- Short PINS are allowed
- Encryption key length is negotiable
- Unit key is reusable and becomes public once used
- The master key is shared
- No user authentication exists
- Unit key sharing can lead to eavesdropping
- End-to-end security is not performed
- Security services are limited

Bluetooth Attacks

Bluejacking

BlueSpam

Blue snarfing

BlueBug Attack

Short Pairing Code Attacks

Man-In-Middle Attacks

BTKeylogging attack

BTVoiceBugging attack

Blueprinting

Bluesmacking

Denial-of-service attack

EC-Council

Bluejacking

Bluejacking is the art of sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as PDA and mobile phones

A loophole in the initialization stage of the Bluetooth communication protocol enables this attack

Before starting the communication, both the Bluetooth devices exchange information during an initial handshake period

In this period, initiating Bluetooth device name is necessary to be displayed on other device's screen

Initiating device sends a user defined field to the target device

An attacker hacks and uses this field to send the unsolicited messages on the target device

BlueSpam finds out the other bluetooth enabled devices and sends a file to them (spam them)

BlueSpam is sent using the OBEX protocol

The file ranges from VCFs (electronic business cards) to simple ASCII text files, images files, audio, and video files

Attacker should have palm with an SD/MMC card to customize the message that should be sent, he/she then creates a directory /PALM/programs/BlueSpam/Send/ and puts the file in it

BlueSpam supports backfire, if it finds any palm into discoverable and connectable mode, BlueSpam intercepts all connection attempts of other Bluetooth devices and starts sending messages back to sender

CEH Certified Ethical Hacker

BlueSnarf™

Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection

For this attack, attacker requires to connect to the OBEX Push Profile (OPP), which is used to exchange information between wireless devices

Attacker connects to the OBEX Push target and performs an OBEX GET request for known filenames such as 'telecom/pb.vcf' for the devices phone book or 'telecom/cal.vcs' for the devices calendar file

If the device is not implemented properly, attacker can gain access to all the files

EC-Council

Bluebug is the loophole in the Bluetooth security

Attacker exploits this loophole and gets unauthorized access to the Bluetooth enabled device

After getting unauthorized access, attacker can:

- Set call forwards
- Read SMS from the phone
- Send SMS to any number
- Initiate phone calls
- Write phonebook entries
- Connect to the Internet
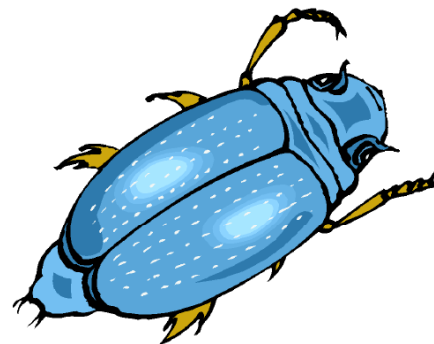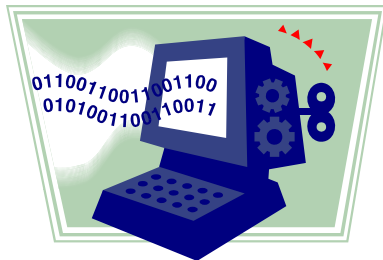
Pairing is a part of Bluetooth, where two devices associate themselves with one another

Those devices share some secret, which is used for future communication

Attacker forces a pair of Bluetooth devices to repeat the pairing process and eavesdrop on it

Attacker pretends to be one of the two devices and sends a message to other claiming to have forgotten the link key

Another device discards the key and creates the new pairing session

With this attack, attacker can eavesdrop on other's Bluetooth network
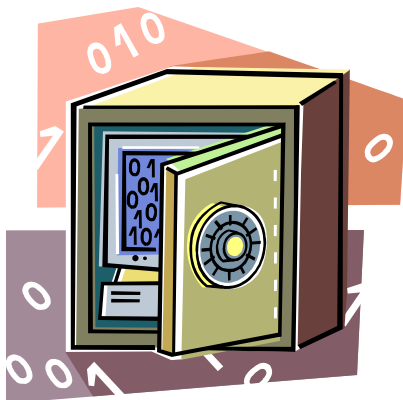
Man-in-the-middle attack is conducted on the Bluetooth link between the laptop and the mobile station

Aim of the attacker is to connect the victim's laptop to a fake WLAN Access Point (AP)

Attacker uses the device which receives the Bluetooth packets in promiscuous mode and then sends forged ones to the mobile and the laptop of the victim

Attack is carried out in two phases:

Recording the Bluetooth session

- Attacker records the Bluetooth session during which the victim's mobile sends the MSK (Master Session Key) to the victim's laptop
- Attacker can also obtain the MSK by compromising the access point used by the victim

Replaying the Bluetooth session

- Attacker forces the laptop to use the compromised MSK by replaying the session recorded during the first phase
- Victim laptop connects to the attacker's access point that uses the compromised MSK
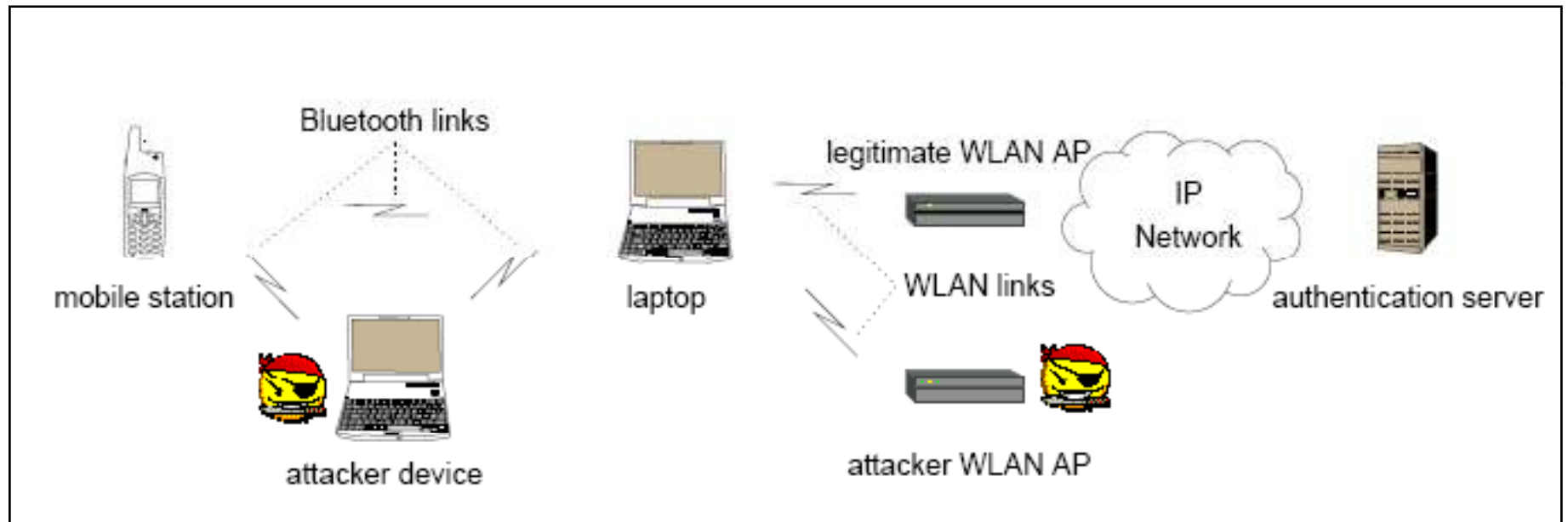
In Online PIN cracking attack, attacker tries to authenticate target device by guessing different PIN values

This attack is possible only if the device has fixed PIN code

For this attack, attacker must know the BD_ADDR of the target device

BD_ADDR is the structure used by all Bluetooth stack layers to identify the address of a Bluetooth device

Security analysis tools used by attacker for OnLine PIN Cracking are:

- OnLine PIN Cracking script
- BruteForce BD_ADDR Scanning script

BTKeylogging attack is possible if the target keyboard has a fixed PIN code and attacker knows its BD_ADDR

Attacker uses PIN Cracking attack to discover the fixed PIN code of the target Bluetooth keyboard

An attacker must know the initial pairing process between the target keyboard and the target computer

Attacker uses a protocol analyzer to intercept all required information (IN RAND, LK RAND, AU RAND, SRES, and EN RAND

Attacker then uses the keyboard as a keylogger by intercepting all packets

BTVoiceBugging Attack

BTVoiceBugging attack is possible when attacker knows the fixed PIN of target device

Attacker uses protocol analyzer and opens two way real-time SCO/eSCO link with the headset

The headset is used as a bugging device

Blueprinting is the process of remotely finding out the details of Bluetooth enabled device

It helps to find out if there are other Bluetooth enabled devices which are vulnerable

Blueprinting reveals the manufacture's details and model number

EC-Council

Bluetooth enabled devices have restrictions on data packet size

Attacker uses Logical Link Control and Adaptation Layer Protocol (L2CAP) for attack

Attacker creates oversized data packets having a size more than the maximum size allowed and sends it to the victim's device

After accessing such an oversized data packet, the victim's device works according to the likes of the attacker

Denial-of-Service Attack

DoS attacks can be conducted on the Bluetooth radio and communications channel

DoS makes devices unable to access Bluetooth resources or other Bluetooth devices to be able to connect it

Bluetooth device, having maximum active connections, is vulnerable for DoS as it consumes the bandwidth

In this case, attacker pairs with the victim's device to request data and never acknowledge receipt of the packets

The communications link will be generated over the ACL physical link type

ACL will retransmit the packet if it does not receive an acknowledgement receipt

Attacker sends a request for large amount of data

ACL retransmits the same data which blocks the bandwidth on the victim's device making the device unable to communicate with other Bluetooth devices

BlueDumping is the technique which causes Bluetooth device to 'dump' it's stored link key, and gives chance to the attacker to sniff into key exchange process

For BlueDump, the attacker must know the BD_ADDR of a set of paired devices

Attacker spoofs the address of one of the devices and connects to the other

When the victim device requests authentication, the attacker's device will respond with an 'HCI_Link_Key_Request_Negative_Reply'

It causes the target device to delete its own link key and go into pairing mode

EC-Council

Bluetooth Hacking Tools

EC-Council

BTScanner

Btscanner is a tool designed specifically to extract as much information as possible from a Bluetooth device without pairing

A detailed information screen extracts HCI (Host Controller Interface) and SDP (Service Discovery Protocol) information, and maintains an open connection to monitor the RSSI and link quality

Btscanner is based on the BlueZ Bluetooth stack, which is included with recent Linux kernels, and the BlueZ toolset
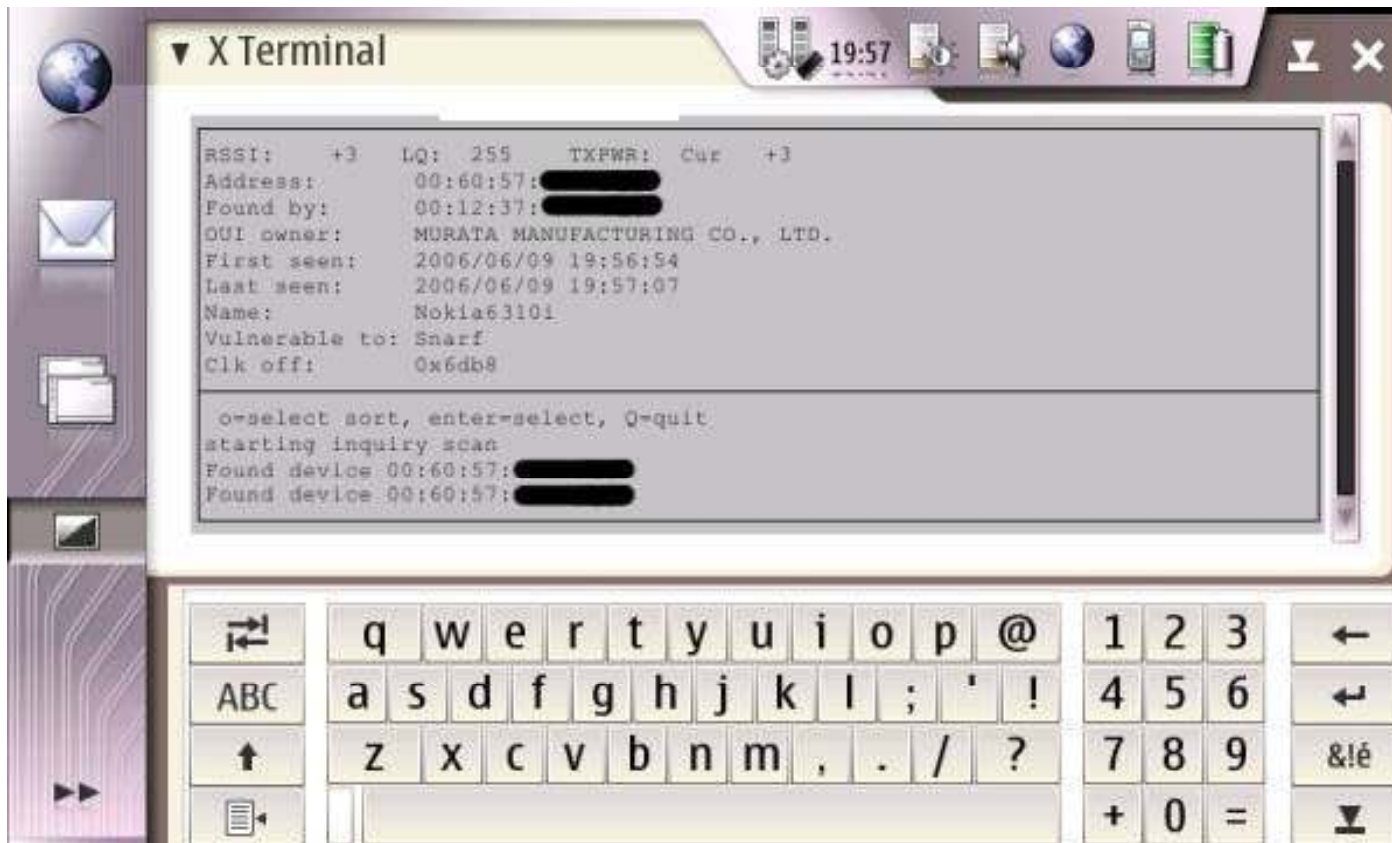
Bluesnarfer downloads the phone-book of any mobile device vulnerable to Bluesnarfing

If a mobile phone is vulnerable, it is possible to connect to the phone without alerting the owner, and gain access to restricted portions of the stored data

EC-Council

Bluesnarfer: Screenshot

Bluediving is a Bluetooth penetration testing suite

It implements attacks like Bluebug, BlueSnarf, BlueSnarf++, and BlueSmack

Features:

- Bluetooth address spoofing
- AT and a RFCOMM socket shell
- Implements tools like carwhisperer, bss, L2CAP packetgenerator, L2CAP connection resetter, and RFCOMM scanner

T-BEAR is a developing suite of applications designed to improve slash "audit" the security of Bluetooth environments

The suite currently consists of the following utilities:

- btsniff: A Bluetooth 'sniffer' for use with gnurado
- btkbsniff: Designed to monitor data from a Bluetooth-enabled keyboard
- btvsniff: Designed to monitor voice data from BT headsets
- btcrackpin: Attempts to crack a PIN associated with encrypted BT data

BTCrack

BTCrack is a Bluetooth PIN and LINK-KEY Cracker

BTCrack reconstructs the PIN and LINK-KEY with data sniffed during a pairing exchange

The calculated PIN can be used to authenticate against a device in Pairing Mode and the LINK-KEY is used to get complete access to the Master and the Slave without any Interaction from the user of these devices

BTCrack: Screenshot
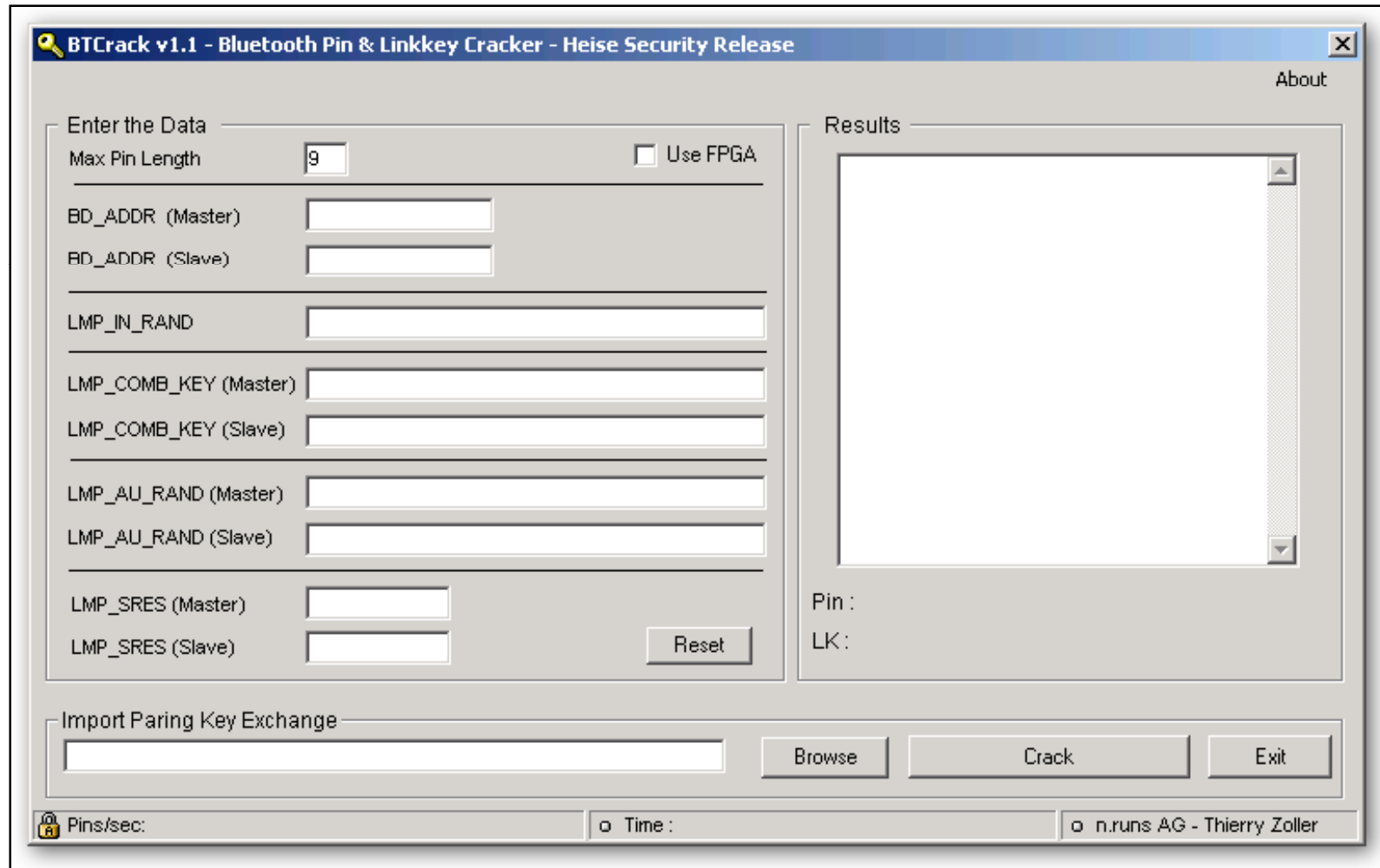
Blooover

Blooover is a tool that is intended to run on J2ME-enabled cell phones that appear to be comparably seamless

Blooover serves as an audit tool that people can use to check whether their phones and phones of friends and employees are vulnerable

Hidattack attacks the Bluetooth human interface driver (HID) protocol

An attacker's Bluetooth scans for a PC in any interesting location, say, in a bank, which has an active Bluetooth HID driver running

Once he finds a victim PC, the attacker's PC becomes a Bluetooth keyboard

The attacker now has full control and therefore can do whatever he wants

Viruses and Worms

Cabir is a Bluetooth-worm that runs in Symbian mobile phones, which supports the Series 60 platform

Cabir replicates over Bluetooth connections

It arrives to the phone's messaging Inbox as a file named caribe.sis containing the worm

When the user clicks caribe.sis and chooses to install the caribe.sis file, the worm activates and starts looking for new devices to infect via Bluetooth

When the Cabir worm finds another Bluetooth device, it will start sending infected SIS files to it, and lock that phone so that it will not look for other phones even when the target moves out of range
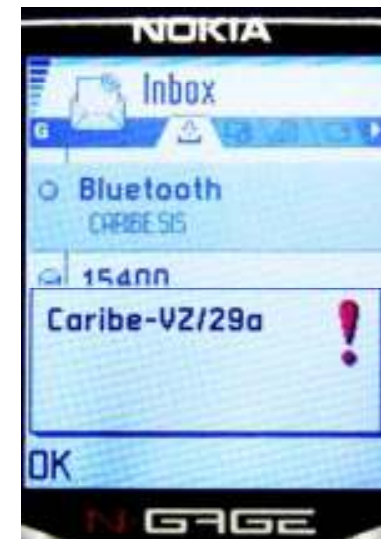
Mabir is a worm that operates on Symbian Series 60 devices

Mabir worm is capable of spreading over both Bluetooth and MMS messages

When Mabir.A infects a phone, it starts searching other phones that in can reach over Bluetooth, and sends infected SIS files to the phones it finds

The SIS files that Mabir.A sends have always the same file name "caribe.sis"

Lasco is a worm capable of infecting PDAs and mobile phones running under Symbian OS

Lasco spreads to executable files (SIS archives) on the infected device

Lasco.a replicates via Bluetooth in the same way as Cabir does

When executing, it scans the disk for SIS archives, and attempts to infect these files found by inserting its code

Installer

Bluetooth
egboy_a920.sis

EGBoy A925

Install Velasco?

?

Yes   No

EC-Council

Bluetooth Security Tools

BlueWatch is the Bluetooth monitoring solution

It identifies all Bluetooth-enabled devices and their communications within a given air space; it also identifies misconfigured devices

It monitors the Bluetooth traffic, and understands Bluetooth-related security threats

Features:

- Identifies different types of Bluetooth devices, including laptops, PDAs, keyboards, and cell phones
- Provides key attributes, including device class, manufacturer, and signal strength
- Illustrates communication or connectivity among various devices
- Identifies services available on each device, including network access, fax, and audio gateway

BlueSweep is a freeware utility to identify and analyze Bluetooth device within a specific range

BlueSweep provides a simple way to gain visibility into your Bluetooth environment and identify related security issues

Features:

Identifies every local Bluetooth device

Sees interconnections between Bluetooth devices
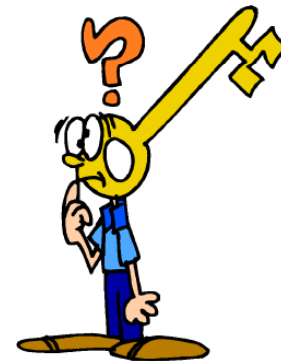
Identifies all services available on each device

EC-Council

Bluekey
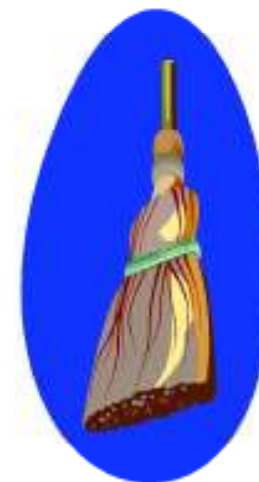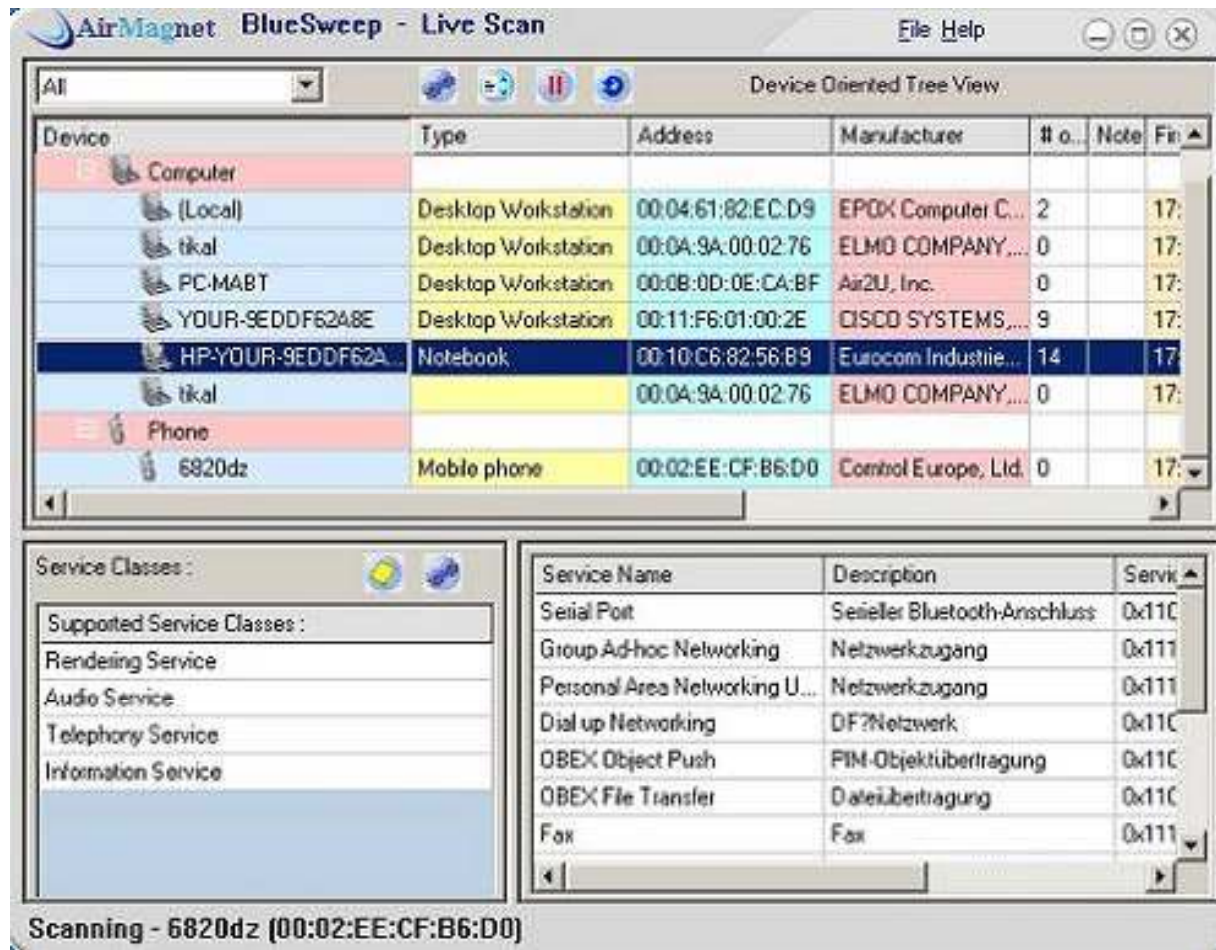
Revolutionary security program that uses Bluetooth

Uses Bluetooth devices to unlock your PDA

Small program for the Palm that adds authentication through Bluetooth device
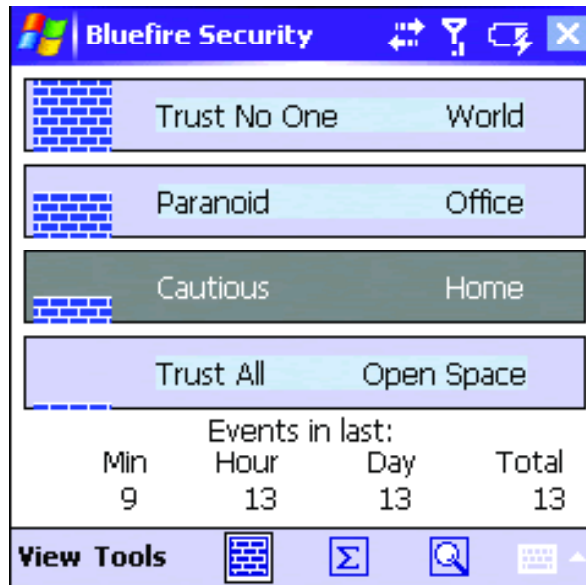
Offers end-to-end wireless solutions for enhancing mobile device functionality

Bluekey

Bluekey: Automated Security
Securing effortlessly... wirelessly

Profile: Default

1   2

Abort

EC-Council

BlueFire Mobile Security Enterprise Edition

BlueFire Mobile Security Enterprise Edition provides network security via an integrated LAN/WAN firewall

Filters traffic to the device in compliance with administrator-controlled port and protocol policies

Intrusion Prevention:

- Scans inbound network packets to identify and prohibit traditional attacks such as LAND

Authentication:

- Enforces power-on PIN or password requirements
- Device wipe allows data residing on the device to be wiped after a set number of failed log-in attempts

Allows administrators to block features including Bluetooth, Speaker/Microphone, USB, IR, Storage Cards, Camera, and ActiveSync

The Integrity Manager can be set to quarantine the device by blocking all incoming and outgoing network communication if an integrity violation has occurred

Captures and retains detailed logs of security events such as successful and invalid login attempts, password resets, quarantine overrides, port scans, firewall activity, and integrity violations

BlueAuditor

BlueAuditor is a tool for detecting and monitoring Bluetooth devices in a wireless network

It can discover and track any Bluetooth device within a distance between 1 and 100 meters and display key information about each device being detected

It enables the user to save the data of the detected Bluetooth devices in an .xml file

It enables network administrators to effectively audit their wireless networks against security vulnerabilities associated with the use of Bluetooth devices
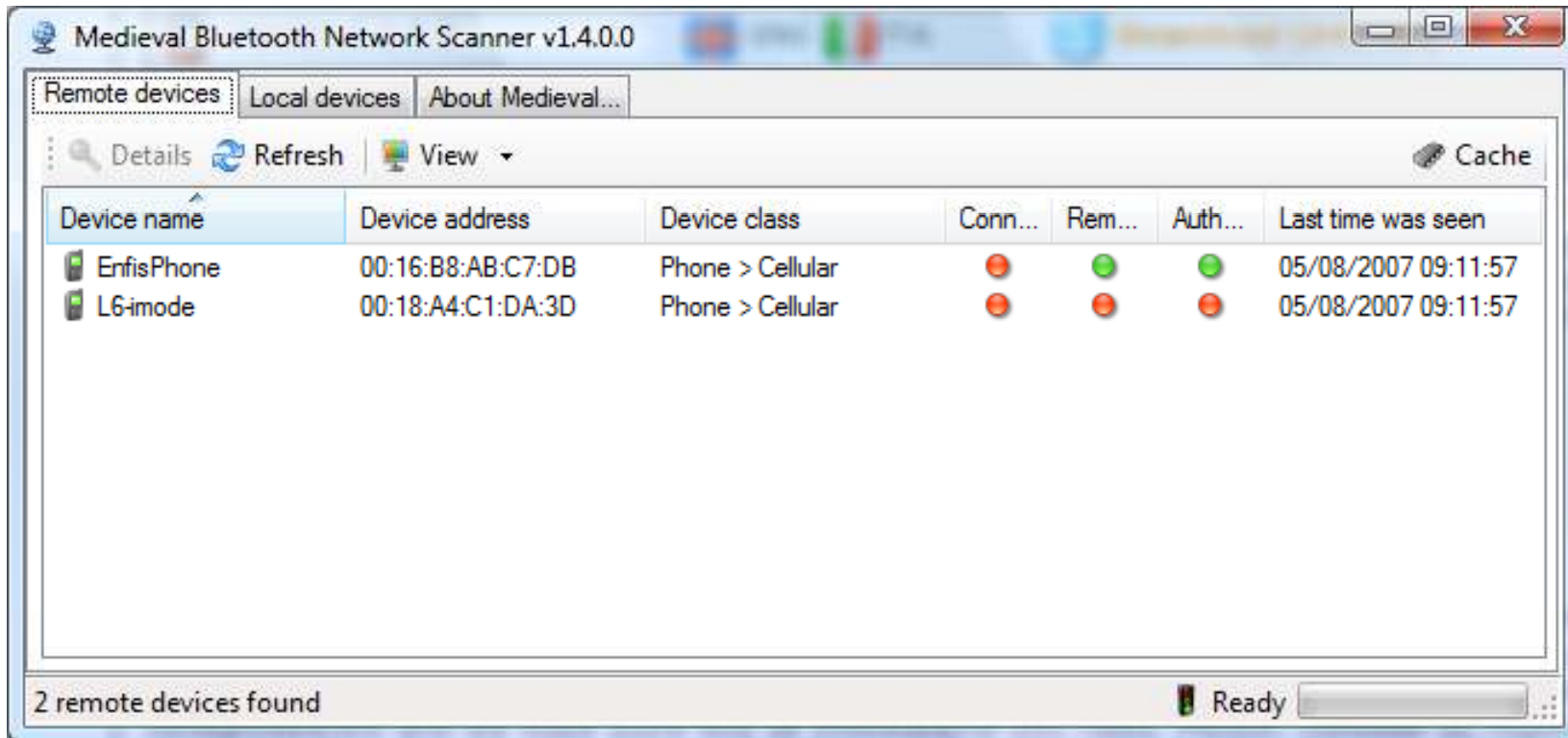
BlueAuditor: Screenshot
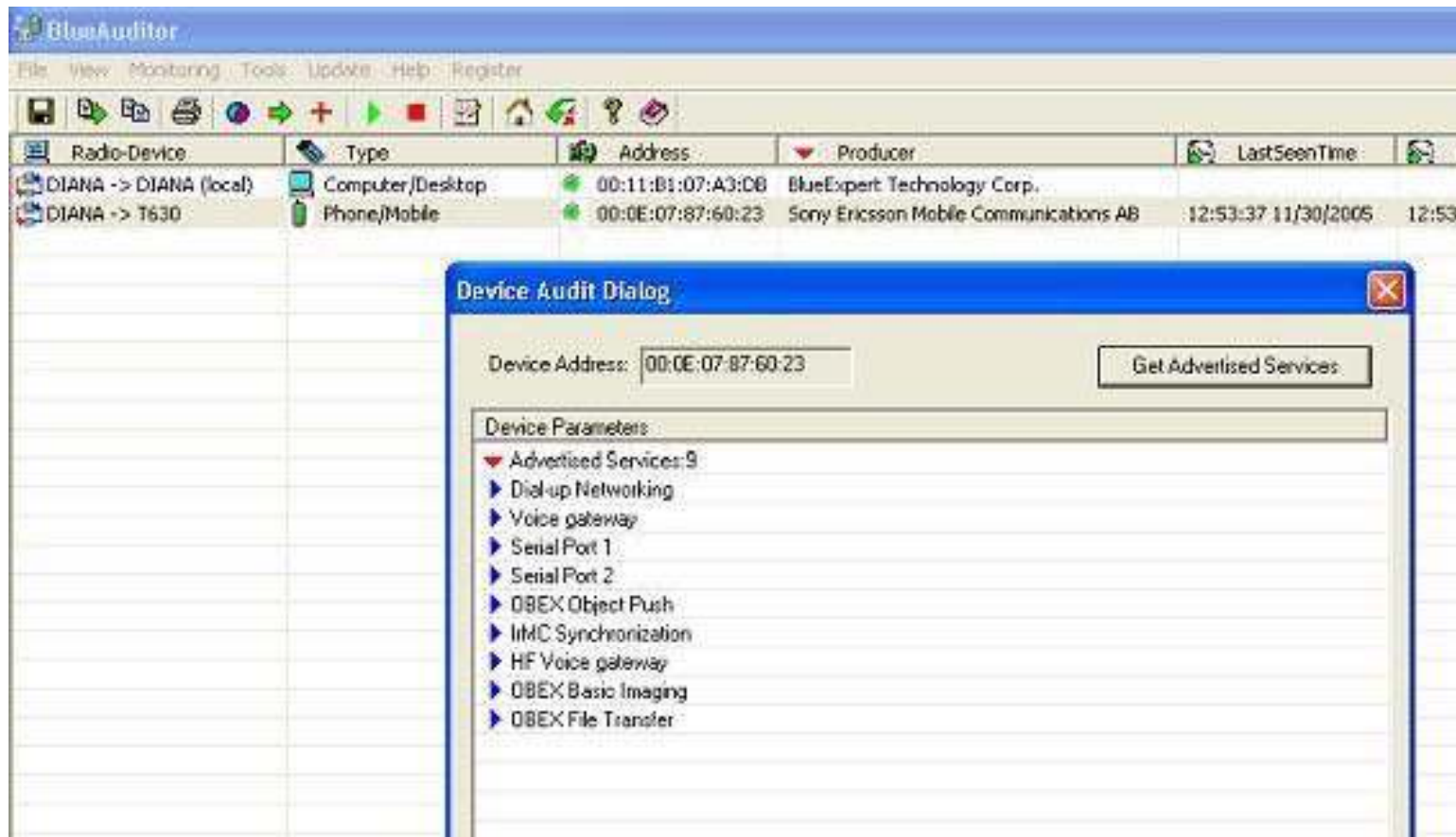
Bluetooth Network Scanner can analyze and scan your Bluetooth network, giving detailed information about local and remote devices found
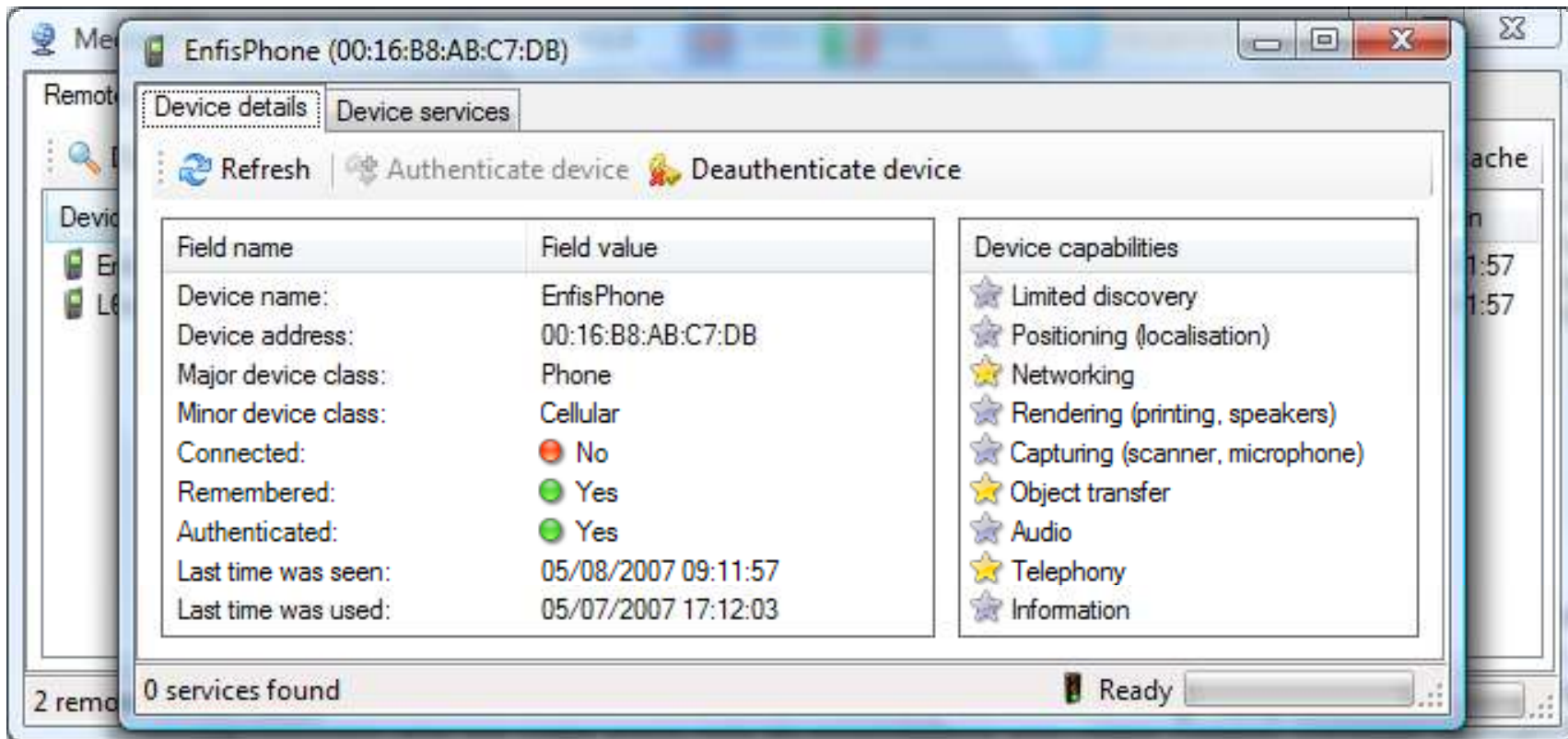
Features:

- Scans both remote devices and local devices
- Explores full details of your phone
- Detects device capabilities along with device information and device address
- You can deeply scan all services of every single Bluetooth device

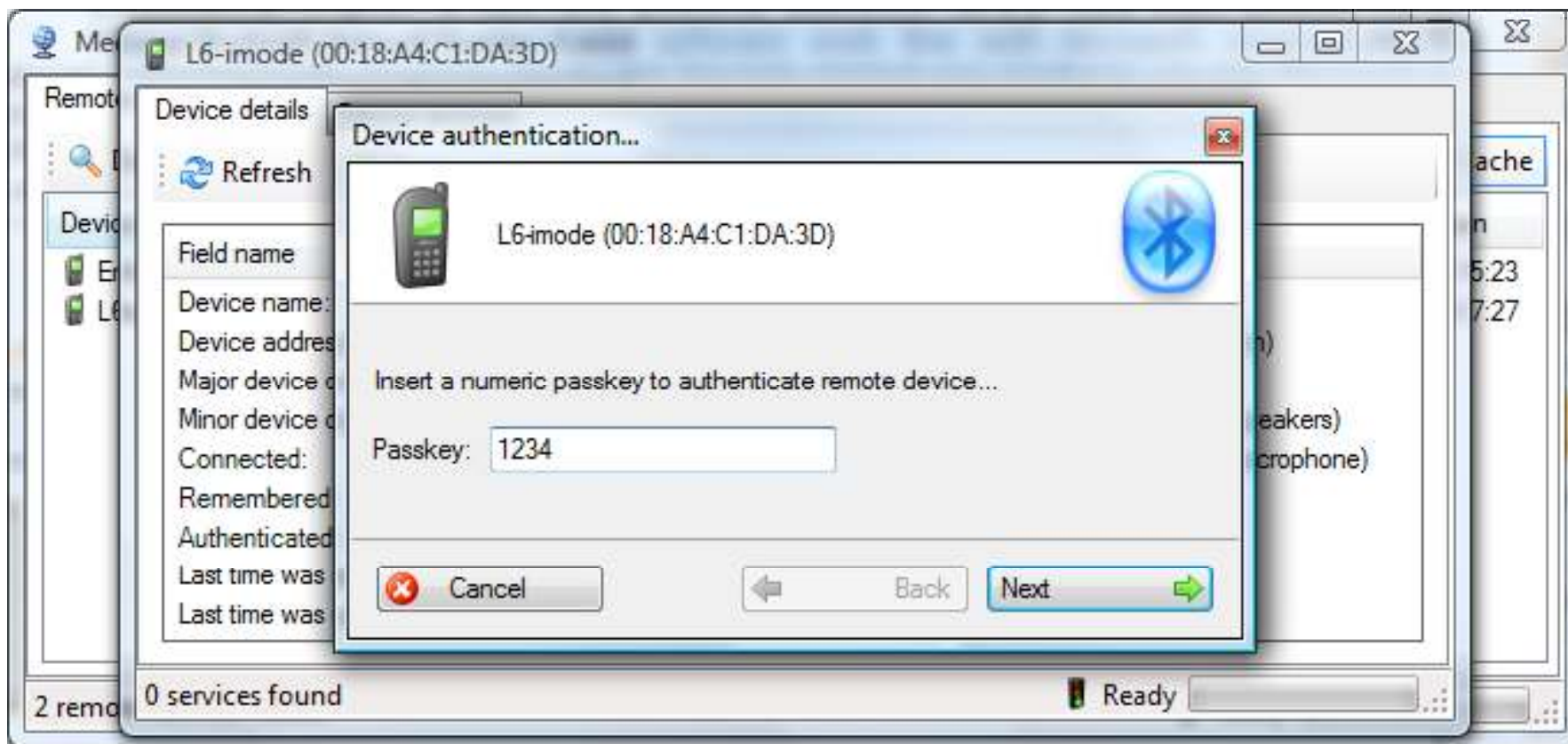# Bluetooth Network Scanner: Screenshot 1

Switch off Bluetooth when not in use

Purchase only devices having long PIN codes

Refrain from entering the PIN into the Bluetooth device for pairing

Limit the electric power itself to keep the range of the network within the physical area

Switch off all unnecessary SCO/eSCO links

Select the proper place when two Bluetooth devices meet for the first time and generate initialization keys

Bluetooth is a short-range wireless communications technology

Bluejacking, BlueSpam, BlueSnarfing, and BlueBug are some of bluetooth attacks

BlueDumping is the technique which causes Bluetooth device to 'dump' it's stored link key, and gives chance to the attacker to sniff into key exchange process

Cabir is a Bluetooth-worm that runs in Symbian mobile phones that support the Series 60 platform

BlueAuditor is a tool for detecting and monitoring Bluetooth devices in a wireless network

"This call may be monitored or recorded because otherwise nobody would believe how stupid some tech support questions can be!"

"Can you show me how to send a Tex message?"